PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2002-229608
(43)Date of publication of application : 16.08.2002

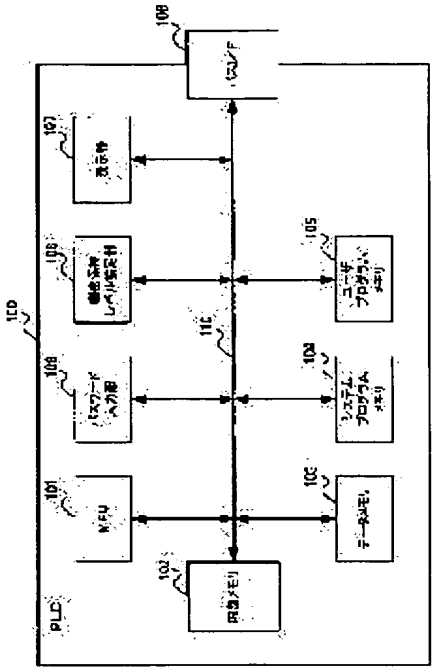
(51)Int.Cl. G05B 19/048
G06F 1/00
G06F 12/14

(21)Application number : 2001-024328
(22)Date of filing : 31.01.2001

(71)Applicant : OMRON CORP
(72)Inventor : IMAI KEISUKE

(54) PROGRAMMABLE CONTROLLER AND CONTROLLING METHOD THEREFOR

(57)Abstract:
PROBLEM TO BE SOLVED: To provide a controlling method for programmable controller allowing a user to individually set a secrecy level according to a use of the user.
SOLUTION: In the programmable controller 100 for controlling secrecy by inputting a password from a password inputting part 109, an allowable number of times of input mistakes of the password and a restoring condition (time till restoring to a state for permitting a re-input of the password) are set in a secrecy level setting part 108, the reception of the password from the password inputting part 109 is inhibited when the number of times of input mistakes of the password from the password inputting part 109 exceeds the allowable number of times set in the secrecy level setting part 108 and subsequently the acceptance inhibiting state of the password is unlocked and the password is accepted only when the restoring condition is satisfied.



(19)日本国特許庁（ＪＰ）　(12)**公開特許公報**（Ａ）　(11)特許出願公開番号
特開2002－229608
（P2002－229608A）
(43)公開日　平成14年８月16日(2002.8.16)

(51)Int.Cl.⁷	識別記号	ＦＩ	テーマコード（参考）
Ｇ０５Ｂ　19/048		Ｇ０６Ｆ　12/14	３２０Ｃ　５Ｂ０１７
Ｇ０６Ｆ　1/00		Ｇ０５Ｂ　19/05	Ｎ　５Ｂ０７６
12/14	３２０	Ｇ０６Ｆ　9/06	６６０Ｅ　５Ｈ２２０

審査請求　未請求　請求項の数６　ＯＬ　（全７頁）

(21)出願番号　特願2001－24328(P2001－24328)

(22)出願日　平成13年１月31日(2001.1.31)

(71)出願人　000002945
オムロン株式会社
京都市下京区塩小路通堀川東入南不動堂町801番地

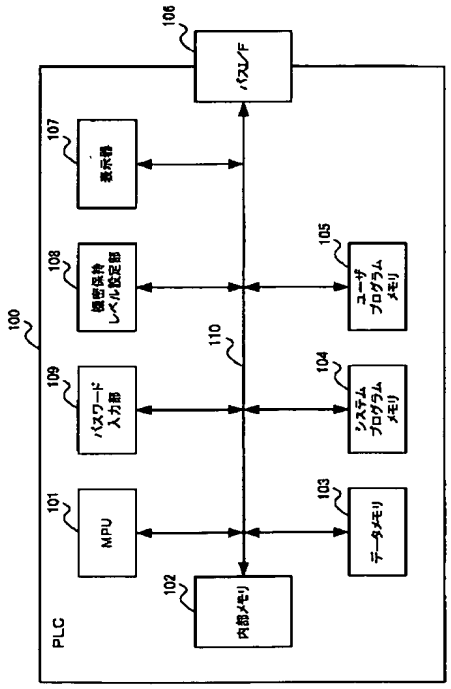
(72)発明者　今井　敬祐
京都府京都市下京区塩小路通堀川東入南不動堂町801番地　オムロン株式会社内

(74)代理人　100069431
弁理士　和田　成則

Ｆターム(参考)　5B017 AA07 BA05 CA16
5B076 FB01
5H220 BB09 CC05 CX06 JJ12 JJ28
JJ34 KK04 LL04 MM10

(54)【発明の名称】　プログラマブルコントローラおよびその制御方法

(57)【要約】
【課題】　ユーザの使用用途に合わせてその機密保持レベルをユーザが個別に設定することができるようにしたプログラマブルコントローラの制御方法を提供する。
【解決手段】　パスワード入力部１０９からのパスワードの入力により機密保持を管理するプログラマブルコントローラ１００において、パスワードの入力ミスの許容回数と復旧条件（パスワードの再入力を許可する状態に復旧するまでの時間）を機密保持レベル設定部１０８で設定し、パスワード入力部１０９からのパスワードの入力ミスの回数が機密保持レベル設定部１０８で設定した許容回数を越えた場合は、パスワード入力部１０９からのパスワードの受付を禁止し、その後は、上記復旧条件が満たされた場合に初めて、パスワードの受付け禁止状態が解除されて当該パスワードの受付けが許容されるものとする。



1

【特許請求の範囲】
【請求項１】　パスワードの入力により機密保持を管理するプログラマブルコントローラにおいて、
上記パスワードの入力ミスの許容条件をユーザにて設定可能とする許容条件設定手段と、
上記パスワードの入力ミスが上記許容条件設定手段で設定された許容条件を越えた場合に、上記パスワードの受付けを禁止する禁止手段とを具備することを特徴とするプログラマブルコントローラ。
【請求項２】　パスワードの入力により機密保持を管理するプログラマブルコントローラにおいて、
上記パスワードの受付け禁止状態を受付け許容状態に戻すための復旧条件をユーザにて設定可能とする復旧条件設定手段と、
上記復旧条件設定手段によって設定された復旧条件が満たされた場合に、上記パスワードの受付け禁止状態を解除し受付け許容状態に戻す解除手段とを具備することを特徴とするプログラマブルコントローラ。
【請求項３】　上記復旧条件は、
上記パスワードの受付けが禁止されてから上記パスワードの受付けを許容する状態に復旧するまでの時間で設定されることを特徴とする請求項２に記載のプログラマブルコントローラ。
【請求項４】　パスワードの入力により機密保持を管理するプログラマブルコントローラの制御方法において、
上記パスワードの入力ミスの許容条件をユーザが設定し、
上記パスワードの入力ミスが上記許容条件を越えた場合は、上記パスワードの受付を禁止することを特徴とするプログラマブルコントローラの制御方法。
【請求項５】　パスワードの入力により機密保持を管理するプログラマブルコントローラの制御方法において、
上記パスワードの受付け禁止状態を受付け許容状態に戻すための復旧条件をユーザが設定し、
上記復旧条件設定手段によって設定された復旧条件が満たされた場合は、上記パスワードの受付け禁止状態を解除し受付け許容状態に戻すことを特徴とするプログラマブルコントローラの制御方法。
【請求項６】　上記復旧条件は、
上記パスワードの受付けが禁止されてから上記パスワードの受付けを許容する状態に復旧するまでの時間で設定されることを特徴とする請求項５に記載のプログラマブルコントローラの制御方法。
【発明の詳細な説明】
【０００１】
【発明の属する技術分野】この発明は、パスワードの入力により機密保持を管理するプログラマブルコントローラおよびその制御方法に関し、特に、ユーザの使用用途に合わせてその機密保持レベルをユーザが個別に設定することができるようにしたプログラマブルコントローラおよびその制御方法に関する。

2

【０００２】
【従来の技術】一般に、プログラマブルコントローラ（ＰＬＣ）は、ユーザプログラム等の機密保持を管理するために特定の情報をパスワードで保護するパスワード機能が設けられている。
【０００３】例えば、パスワードを用いて特定のユーザプログラムのリードプロテクトを行う場合は、この特定のユーザプログラムのリードに際して、パスワードの入力が要求され、ここで正しいパスワードが入力されないと、この特定のユーザプログラムのリードが禁止される。
【０００４】ところで、上記パスワードを用いた機密保持管理においても、厳しい管理が要求される場合と、反対に柔軟な管理が要求される場合とがある。
【０００５】一般に、パスワードは、その入力ミスの許容回数を無制限に設定したシステムでは、パスワードの全組み合わせを自動的に入力する装置が用いられると、簡単にパスワードを解読されてしまうので、厳しい管理が要求される場合には、機密保持を設定する機能としては条件を満足しないので、入力ミスの許容回数に制限を与える必要がある。
【０００６】しかし、反対に、柔軟な管理が要求される場合には、例えば、パスワードの入力ミスの許容回数を３回に制限し、パスワードの入力ミスを３回繰り返すとその時点でシステムは復旧不能となるように構成すると、オペレータがパスワードを忘れた場合等で入力ミスを３回しただけで、そのシステムはパスワードを受け付けなくなり、機密保持機能としては厳しすぎることになる。
【０００７】さて、最近、プログラマブルコントローラにおいて、ユーザプログラムの機密保持の要求は多くなってきている。また、プログラマブルコントローラの使う用途も多様化しており、パスワードによる機密保持レベルをシステムとして一意に決めることができなくなっている。
【０００８】したがって、ユーザが使用用途に合わせて機密保持レベルを設定できるようにすることはシステムを提供するメーカ側および提供されるユーザ側にとって非常に有用である。
【０００９】しかしながら、従来のプログラマブルコントローラにおいては、パスワードのリードプロテクトの設定を行った場合、パスワードの入力ミスの許容回数およびパスワードの入力ミスの許容回数を越えた場合のシステムの復旧方法は予めシステムにて決められていた。
【００１０】図５は、従来のプログラマブルコントローラにおけるパスワードの処理手順を示すフローチャートである。
【００１１】図５において、パスワードがプログラマブルコントローラに入力されると（ステップ５０１）、ま

ず、この入力されたパスワードが正しいか、すなわち、この入力されたパスワードがこのプログラマブルコントローラに予め設定されているパスワードと一致するかが調べられる（ステップ５０２）。

【００１２】ここで、パスワードが一致したと判断されると（ステップ５０２でＹＥＳ）、このプログラマブルコントローラにパスワードが受理され（ステップ５０５）、例えば、このプログラマブルコントローラのユーザプログラムのリードが許可される。

【００１３】しかし、ステップ５０２で、パスワードが一致しないと判断されると（ステップ５０２でＮＯ）、次に、パスワードが一致しない入力ミスの回数が予めシステムに設定されたｎ回（例えば３回）に達したかが調べられる（ステップ５０３）。

【００１４】ここで、パスワードの入力ミスがｎ回に達していないと判断されると（ステップ５０３でＮＯ）、ステップ５０１に戻り、パスワードの再入力が許容される。

【００１５】しかし、ステップ５０３でパスワードの入力ミスがｎ回に達したと判断されると（ステップ５０３でＹＥＳ）、このパスワードは無効にされ（ステップ５０４）、そのシステムはパスワードを受け付けなくなる。

【００１６】このように従来のプログラマブルコントローラのパスワード処理手順においては、その機密保持レベルがシステムにより一義的に決定され、例えば、パスワードの入力ミスの回数がシステムに設定された所定回数に達すると、このプログラマブルコントローラは動作不能になり、その後の処理ができなくなるという問題があった。

【００１７】

【発明が解決しようとする課題】そこで、この発明は、ユーザの使用用途に合わせてその機密保持レベルをユーザが個別に設定することができるようにして柔軟なパスワードの運用ができるようにすることを目的とする。

【００１８】また、この発明は、ユーザの使用用途に合わせてその機密保持レベルをユーザが個別に設定することができ、ユーザ側で柔軟なパスワードの運用を行えるようにしたプログラマブルコントローラを提供することを目的とする。

【００１９】また、この発明は、ユーザの使用用途に合わせてその機密保持レベルをユーザが個別に設定することができ、ユーザ側で柔軟なパスワードの運用を行えるようにしたプログラマブルコントローラの制御方法を提供することを目的とする。

【００２０】

【課題を解決するための手段】この発明に係るプログラマブルコントローラは、パスワードの入力により機密保持を管理するプログラマブルコントローラにおいて、上記パスワードの入力ミスの許容条件をユーザにて設定可能とする許容条件設定手段と、上記パスワードの入力ミスが上記許容条件設定手段で設定された許容条件を越えた場合に、上記パスワードの受付けを禁止する禁止手段とを具備することを特徴とする。

【００２１】また、この発明に係るプログラマブルコントローラは、パスワードの入力により機密保持を管理するプログラマブルコントローラにおいて、上記パスワードの受付け禁止状態を受付け許容状態に戻すための復旧条件をユーザにて設定可能とする復旧条件設定手段と、上記復旧条件設定手段によって設定された復旧条件が満たされた場合に、上記パスワードの受付け禁止状態を解除し受付け許容状態に戻す解除手段とを具備することを特徴とする。

【００２２】この発明に係るプログラマブルコントローラの制御方法は、パスワードの入力により機密保持を管理するプログラマブルコントローラの制御方法において、上記パスワードの入力ミスの許容条件をユーザが設定し、上記パスワードの入力ミスが上記許容条件を越えた場合は、上記パスワードの受付を禁止することを特徴とする。

【００２３】また、この発明に係るプログラマブルコントローラの制御方法は、パスワードの入力により機密保持を管理するプログラマブルコントローラの制御方法において、上記パスワードの受付け禁止状態を受付け許容状態に戻すための復旧条件をユーザが設定し、上記復旧条件設定手段によって設定された復旧条件が満たされた場合は、上記パスワードの受付け禁止状態を解除し受付け許容状態に戻すことを特徴とする。

【００２４】ここで、上記入力ミスの許容条件は、上記パスワードの入力ミスの回数で設定することができる。

【００２５】また、上記復旧条件は、上記パスワードの受付けが禁止されてから上記パスワードの受付けを許容する状態に復旧するまでの時間で設定することができる。

【００２６】

【発明の実施の形態】以下、この発明に係わるプログラマブルコントローラおよびその制御方法の実施の形態について添付図面を参照して詳細に説明する。

【００２７】図１は、この発明に係わるプログラマブルコントローラの概略構成を示すブロック図である。

【００２８】図１において、このプログラマブルコントローラ（ＰＬＣ）１００は、ＭＰＵ(Micro Processing Unit)１０１、内部メモリ１０２、データメモリ１０３、システムプログラムメモリ１０４、ユーザプログラムメモリ１０５、バスＩ／Ｆ（バスインターフェース）１０６、表示器１０７、機密保持レベル設定部１０８、パスワード入力部１０９をシステムバス１１０で相互に接続して構成される。

【００２９】ここで、ＭＰＵ１０１は、このプログラマブルコントローラ１００の全体動作を制御するものであ

る。

【００３０】内部メモリ１０２は、プログラマブルコントローラ１００の内部データを格納するものであり、データメモリ１０３は、各種データを記憶するものである。この発明に係るプログラマブルコントローラ１００に設定されたパスワードは、プログラマブルコントローラ１００に固有のものとして、このデータメモリ１０３に存在するものであってもよいし、ユーザプログラムの一部としてユーザプログラムメモリ１０５に存在するものであってもよい。

【００３１】システムプログラムメモリ１０４には、このプログラマブルコントローラ１００のシステムプログラムが格納され、ユーザプログラムメモリ１０５には、このプログラマブルコントローラ１００のユーザが使用するユーザプログラムが格納されている。

【００３２】バスＩ／Ｆ１０６は、システムバス１１０とのインタフェースをなすもので、図示しないＩ／Ｏユニット、高機能ユニット等はこのバスＩ／Ｆ１０６を介して接続される。

【００３３】表示器１０７は、ＬＣＤ(Liquid Crystal Display)から構成され、このプログラマブルコントローラ１００の動作に係わる各種情報を表示するものである。

【００３４】パスワード入力部１０９は、複数のキースイッチから構成され、パスワードを入力するものである。

【００３５】機密保持レベル設定部１０８は、パスワードの入力ミスの許容条件をユーザにて設定可能とする許容条件設定手段、および、パスワードの受付け禁止状態を受付け許容状態に戻すための復旧条件をユーザにて設定可能とする復旧条件設定手段として機能するものであり、その設定条件や復旧条件の具体的な内容については後述の通りである。

【００３６】この実施の形態のプログラマブルコントローラ１００においては、機密保持レベル設定部１０８でユーザにより設定されたパスワードの入力ミス許容条件および復旧条件に基づき、パスワードの機密保持がこのプログラマブルコントローラ１００の用途に対応して柔軟に制御される。

【００３７】パスワードの入力ミスの許容条件は、パスワード入力部１０９からのパスワードの入力ミスの許容条件であり、ここでは、入力ミスの回数で設定される。

【００３８】復旧条件は、時間で設定される。この復旧条件の時間は、パスワード入力部１０９から入力されたパスワードの入力ミス回数が入力ミス許容条件を越えることで、当該パスワードの受付けが禁止された時点から、再びパスワードの受付けを許容する状態、すなわちパスワードの再入力を許可する状態に復旧するまでの時間である。

【００３９】この実施の形態のプログラマブルコントローラ１００においては、上記のような入力ミスの許容条件と復旧条件の両者でこのプログラマブルコントローラ１００の機密保持レベルを設定している。

【００４０】入力ミスの許容条件（本実施形態ではパスワードの入力ミス回数）の設定については、入力ミス回数に制限を設けない無制限の設定、または０回、１回または５回等のように入力ミス回数を制限する設定が可能である。

【００４１】復旧条件（本実施形態ではパスワードの再入力を許可する状態に復旧するまでの時間）の設定については、無しから最小単位時間までの設定が可能である。

【００４２】上記のような入力ミスの許容条件の設定と復旧条件の設定は、ユーザ側で用途に応じて任意に行える。したがって、機密保持レベルをどの程度のものとするかの判断はユーザに委ねられており、ユーザとしては用途に適した任意の機密保持レベルを独自にかつ自由に設定することができる。

【００４３】機密保持レベルの高低感はユーザの意識にもよるが、その機密保持レベルの程度とそのレベルの内容を以下に例示する。

【００４４】プログラマブルコントローラ１００において、機密保持レベルを「低」レベルに設定したい場合には、入力ミスの許容条件を無制限に設定する。この場合は、パスワードの入力ミスを何回繰り返しても、パスワードの再入力が可能であり、比較的低い機密保持レベルでもよい場合に好適である。

【００４５】また、機密保持レベルを「中」レベルに設定したい場合は、例えば、入力ミスの許容条件を５回、復旧条件を２時間に設定する。この場合は、パスワードの入力ミスを５回繰り返すと、パスワードの再入力ができなくなり、この状態からパスワードの再入力を可能な状態に復旧させるためには２時間待たなければならず、したがって、この例は上記例より上の機密保持レベルを必要とする場合に好適である。

【００４６】さらに、機密保持レベルを「高」レベルに設定したい場合は、例えば、入力ミスの許容条件は１回に設定し、復旧条件は無しに設定する。この場合は、パスワードの入力ミスを１回行うと、パスワードの再入力ができなくなり、この状態になると、何時間待ってもパスワードの再入力を可能な状態に復旧しない。したがって、この例は上記いずれの例よりも上の機密保持レベルを必要とする場合に好適である。

【００４７】図２は、図１に示したプログラマブルコントローラ１００におけるパスワードの処理手順を示すフローチャートである。

【００４８】図２において、図１に示したパスワード入力部１０９からこのプログラマブルコントローラ１００にパスワードが入力されると（ステップ２０１）、まず、この入力されたパスワードが正しいか、すなわち、

この入力されたパスワードと、このプログラマブルコントローラ１００のデータメモリ１０３またはユーザプログラムメモリ１０５に予め設定されているパスワードとを比較し、その両者が一致するかが調べられる（ステップ２０２）。

【００４９】ここで、パスワードが一致したと判断されると（ステップ２０２でＹＥＳ）、このプログラマブルコントローラ１００にパスワードが受理され（ステップ２０７）、例えば、このプログラマブルコントローラ１００のユーザプログラムメモリ１０５に格納された特定のユーザプログラムのリードが許可される。

【００５０】しかし、ステップ２０２で、パスワードが一致しないと判断されると（ステップ２０２でＮＯ）、次に、パスワードが一致しない入力ミスの回数が機密保持レベル設定部１０８で設定された入力ミス許容回数ｎ（例えば５回）に達したかが調べられる（ステップ２０３）。

【００５１】ここで、パスワードの入力ミスがｎ回に達していないと判断されると（ステップ２０３でＮＯ）、ステップ２０１に戻り、パスワードの再入力が許容される。

【００５２】しかし、パスワードの入力ミスが何度も続き、ステップ２０３でパスワードの入力ミスがｎ回に達したと判断されると（ステップ２０３でＹＥＳ）、パスワードの不受理状態に制御され（ステップ２０４）、次に、機密保持レベル設定部１０８で設定された復旧時間ｔが経過したかが調べられる（ステップ２０５）。

【００５３】ここで、復旧時間ｔが経過していないと判断されると（ステップ２０５でＮＯ）、ステップ２０５に戻る。この間、パスワードの不受理状態は継続される。

【００５４】しかし、ステップ２０５で、復旧時間ｔが経過したと判断されると（ステップ２０５でＹＥＳ）、パスワード不受理状態を解除し（ステップ２０６）、ステップ２０１に戻り、パスワードの再入力が許容される。

【００５５】ところで、上記復旧時間ｔは、プログラマブルコントローラ１００の電源がオフにされるとリセットされ、電源オン後に再びｔ時間の計時が開始されるように構成することもできる。

【００５６】図３は、このように構成されたパスワードの処理手順を示すフローチャートである。

【００５７】図３において、図１に示したパスワード入力部１０９からこのプログラマブルコントローラ１００にパスワードが入力されると（ステップ３０１）、まず、この入力されたパスワードが正しいか、すなわち、この入力されたパスワードがこのプログラマブルコントローラ１００のデータメモリ１０３に予め設定されているパスワードと一致するかが調べられる（ステップ３０２）。

【００５８】ここで、パスワードが一致したと判断されると（ステップ３０２でＹＥＳ）、このプログラマブルコントローラ１００にパスワードが受理され（ステップ３１０）、例えば、このプログラマブルコントローラ１００のユーザプログラムメモリ１０５に格納された特定のユーザプログラムのリードが許可される。

【００５９】しかし、ステップ３０２で、パスワードが一致しないと判断されると（ステップ３０２でＮＯ）、次に、パスワードが一致しない入力ミスの回数が機密保持レベル設定部１０８で設定された入力ミスの許容回数ｎ（例えば５回）に達したかが調べられる（ステップ３０３）。

【００６０】ここで、パスワードの入力ミスがｎ回に達していないと判断されると（ステップ３０３でＮＯ）、ステップ３０１に戻り、パスワードの再入力が許容される。

【００６１】しかし、ステップ３０３でパスワードの入力ミスがｎ回に達したと判断されると（ステップ３０３でＹＥＳ）、パスワードの不受理状態に制御され（ステップ３０４）、次に、プログラマブルコントローラ１００内に設けられたタイマをスタートさせる（ステップ３０５）。

【００６２】そして、次に、このタイマの計時時間が機密保持レベル設定部１０８で設定された復旧時間ｔが経過したかが調べられる（ステップ３０６）。

【００６３】ここで、復旧時間ｔが経過したと判断されると（ステップ３０６でＹＥＳ）、パスワード不受理状態を解除し（ステップ３０９）、ステップ３０１に戻り、パスワードの再入力が許容される。

【００６４】しかし、ステップ３０６で復旧時間ｔが経過していないと判断されると（ステップ３０６でＮＯ）、計時を続ける。

【００６５】図４は、上記図３に示したパスワード処理手順のステップ３０６でｔ時間経過待ちを実行中にプログラマブルコントローラ１００の電源がオフされた場合の動作を説明する図である。

【００６６】図４において、パスワードの一致が得られず、時点ｔ１で図３のステップ３０５に示すタイマがスタートしたが、このタイマの計時時間が復旧時間ｔに達しない時点ｔ２でプログラマブルコントローラ１００の電源をオフにしたときは、その後に電源をオンにした時点ｔ３で、上記タイマは初期値にリセットされ再スタートされる。したがって、電源をオンにした時点ｔ３から復旧時間ｔが経過する時点ｔ４までの間にパスワードを入力しても、このパスワードは受理されない。

【００６７】そして、電源をオンにした時点ｔ３から復旧時間ｔが経過した時点ｔ４以降において初めてパスワードの受理が可能になる。

【００６８】このような構成によると、例えば、パスワードの一致が得られず、パスワードの不法解析のために

このプログラマブルコントローラ１００の電源をオフにして持ちかえったとしても、電源をオンにした時点でタイマは再スタートされるので、少なくとも、機密保持レベル設定部１０８で設定された復旧時間ｔの間はパスワードを受け付けない。

【００６９】

【発明の効果】以上説明したように、この発明によれば、パスワードの入力により機密保持を管理するプログラマブルコントローラにおいて、ユーザの使用用途に合わせてその機密保持レベルをユーザが個別に設定することができるように構成したので、ユーザ側ではその機密保持を管理するレベルの設定の自由度が高まり、ユーザの使用用途に合わせた柔軟なパスワードの運用が可能になるという効果を奏する。

【図面の簡単な説明】

【図１】この発明に係わるプログラマブルコントローラの概略構成を示すブロック図。

【図２】図１に示したプログラマブルコントローラ１００におけるパスワードの処理手順を示すフローチャート図。

＊【図３】図１に示したプログラマブルコントローラ１００におけるパスワードの他の処理手順を示すフローチャート図。

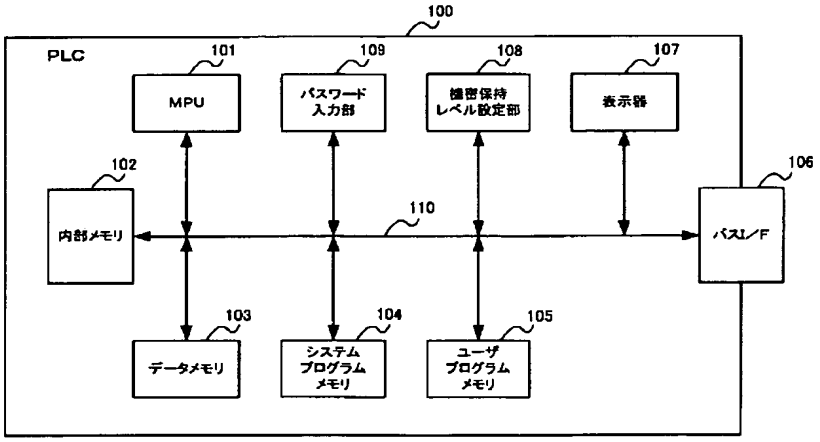
【図４】図３に示したパスワードの処理手順を採用する場合の動作を説明する図。

【図５】従来のプログラマブルコントローラにおけるパスワードの処理手順を示すフローチャート図。

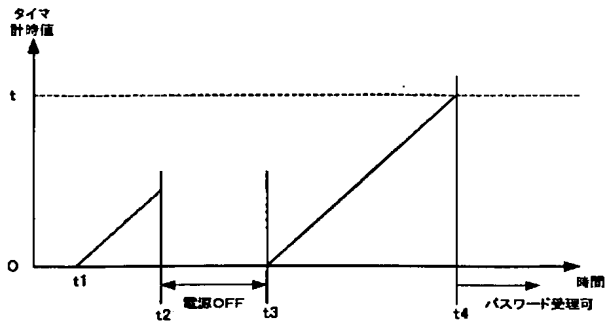
【符号の説明】

１００	プログラマブルコントローラ（ＰＬＣ）
１０１	ＭＰＵ(Micro Processing Unit)
１０２	内部メモリ
１０３	データメモリ
１０４	システムプログラムメモリ
１０５	ユーザプログラムメモリ
１０６	バスＩ／Ｆ（バスインターフェース）
１０７	表示器
１０８	機密保持レベル設定部
１０９	パスワード入力部
１１０	システムバス

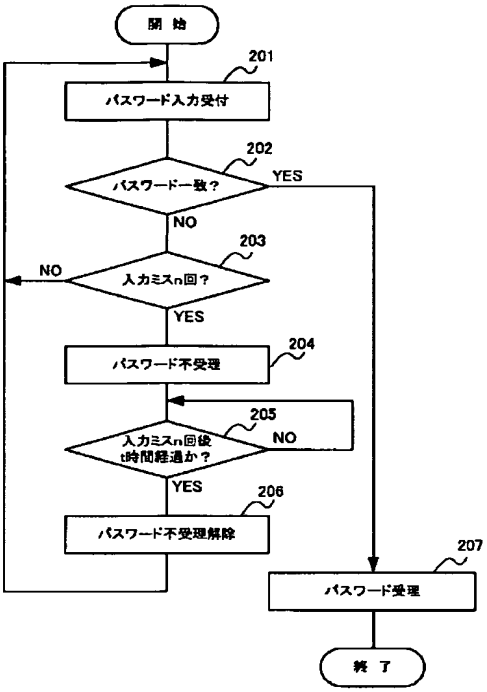
【図１】



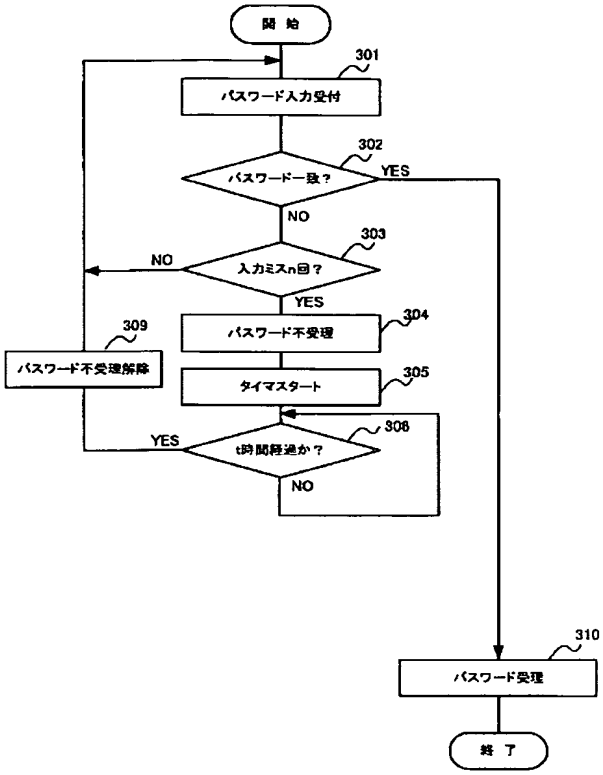
【図４】



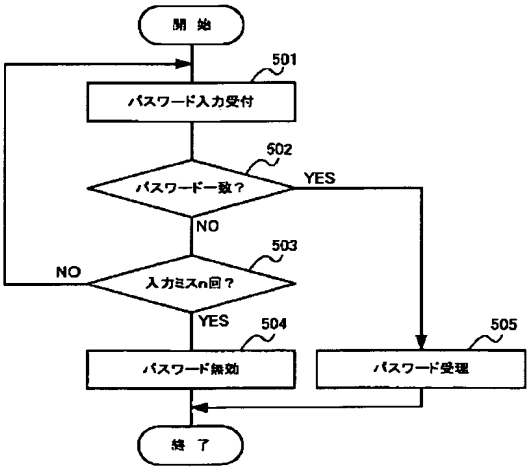
【図２】


開始
201
パスワード入力受付
202
パスワード一致？
YES
NO
203
入力ミスn回？
NO
YES
204
パスワード不受理
205
入力ミスn回後
t時間経過か？
NO
YES
206
パスワード不受理解除
207
パスワード受理
終了

【図３】


開始
301
パスワード入力受付
302
パスワード一致？
YES
NO
303
入力ミスn回？
NO
YES
304
パスワード不受理
305
タイマスタート
306
t時間経過か？
YES
NO
309
パスワード不受理解除
310
パスワード受理
終了

【図５】


開始
501
パスワード入力受付
502
パスワード一致？
YES
NO
503
入力ミスn回？
NO
YES
504
パスワード無効
505
パスワード受理
終了

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

CLAIMS

[Claim(s)]
[Claim 1]A programmable controller which manages security protection by the input of a password, comprising:
A permissive-conditions setting-out means which enables setting out of permissive conditions of an input mistake of the above-mentioned password by a user.
An inhibiting means which forbids registration of the above-mentioned password when an input mistake of the above-mentioned password exceeds permissive conditions set up by the above-mentioned permissive-conditions setting-out means.

[Claim 2]A programmable controller which manages security protection by the input of a password, comprising:
A restoring condition setting-out means which enables setting out of a restoring condition for receiving a receptionist prohibited state of the above-mentioned password, and returning to a permissive condition by a user.
A release means which cancels a receptionist prohibited state of the above-mentioned password, and is returned to a receptionist permissive condition when a restoring condition set up by the above-mentioned restoring condition setting-out means is fulfilled.

[Claim 3]The programmable controller according to claim 2, wherein the above-mentioned restoring condition is set up in time until it restores in the state of permitting registration of the above-mentioned password after registration of the above-mentioned password is forbidden.
[Claim 4]In a control method of a programmable controller of managing security protection by the input of a password, A control method of a programmable controller characterized by forbidding reception of the above-mentioned password when a user sets up permissive conditions of an input mistake of the above-mentioned password and an input mistake of the above-mentioned password exceeds the above-mentioned permissive conditions.
[Claim 5]In a control method of a programmable controller of managing security protection by the input of a password, When a restoring condition which a user set up a restoring condition for receiving a receptionist prohibited state of the above-mentioned password, and returning to a permissive condition, and was set up by the above-mentioned restoring condition setting-out means is fulfilled, A control method of a programmable controller canceling a receptionist prohibited state of the above-mentioned password, and returning to a receptionist permissive condition.
[Claim 6]A control method of the programmable controller according to claim 5, wherein the above-mentioned restoring condition is set up in time until it restores in the state of permitting registration of the above-mentioned password after registration of the above-mentioned password is forbidden.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DETAILED DESCRIPTION

[Detailed Description of the Invention]
[0001]
[Field of the Invention]This invention about a programmable controller which manages security protection by the input of a password, and a method for controlling the same, It is related with a programmable controller with which the user enabled it to set up the security protection level individually especially according to a user's usage, and a method for controlling the same.
[0002]
[Description of the Prior Art]Generally, in order that a programmable controller (PLC) may manage security protection, such as a user program, the password function which protects specific information with a password is provided.
[0003]For example, if the input of a password is required and a right password is not entered when leading this specific user program here when performing lead protection of a specific user program using a password, the lead of this specific user program will be forbidden.
[0004]By the way, also in the security protection management using the above-mentioned password, management flexible on the contrary may be required as the case where severe management is required.
[0005]Generally a password the number of times of permission of the input mistake in the system set up indefinitely. Since conditions are not satisfied as a function to set up security protection when severe management is required, since a password will be simply decoded if the device which inputs a total combination of a password automatically is used, it is necessary to give restriction to the number of times of permission of an input mistake.
[0006]However, when flexible management is required on the contrary. For example, if it constitutes so that a system may be cannot be restored at the time, if the number of times of permission of the input mistake of a password is restricted to 3 times and the input mistake of a password is repeated 3 times, Only by turning an input mistake three by the case where the operator has forgotten the password etc., the system stops receiving a password and will be too severe as a security protection function.
[0007]Now, the demand of the security protection of a user program has been increasing in a programmable controller recently. The use which a programmable controller uses is also diversified and it is impossible to decide on a meaning by using a security protection level with a password as a system.
[0008]Therefore, it is dramatically useful that a user enables it to set up a security protection level according to usage for the maker side which provides a system, and the user side provided.
[0009]However, in the conventional programmable controller, when lead protection of a password was set up, the restoration method of the system at the time of exceeding the number of times of permission of the input mistake of a password and the number of times of permission of the input mistake of a password was beforehand decided by the system.
[0010]Drawing 5 is a flow chart which shows the procedure of the password in the conventional programmable controller.
[0011]In drawing 5, if a password is entered into a programmable controller (Step 501), First, it is investigated whether this entered password of the right, i.e., this entered password, corresponds with the password beforehand set as this programmable controller (Step 502).
[0012]Here, if it is judged that the password was in agreement (it is YES at Step 502), a password will be received by this programmable controller (Step 505), for example, the lead of the user program of this programmable controller will be permitted.
[0013]However, if it is judged at Step 502 that a password is not in agreement (it is NO at Step 502) next, it will be investigated whether the number of times of the input mistake whose password does not correspond

amounted to n times (for example, 3 times) beforehand set as the system (Step 503).
[0014]Here, when it is judged that the input mistake of a password does not amount to n times (it is NO at Step 503), it returns to Step 501 and reinput of a password is permitted.
[0015]When it is judged that the input mistake of the password amounted to n times at Step 503 (it is YES at Step 503), this password is repealed (Step 504) and that system stops however, receiving a password.
[0016]Thus, in the password procedure of the conventional programmable controller, When that security protection level was uniquely determined by the system, for example, the number of times of the input mistake of a password became the prescribed frequency set as the system, this programmable controller became impossible of operation, and there was a problem of subsequent processing becoming impossible.
[0017]
[Problem(s) to be Solved by the Invention]Then, an object of this invention is to be able to be made to perform employment of a flexible password, as a user can set up that security protection level individually according to a user's usage.
[0018]According to a user's usage, a user can set up that security protection level individually, and an object of this invention is to provide the programmable controller which enabled it to employ a flexible password by the user side.
[0019]According to a user's usage, a user can set up that security protection level individually, and an object of this invention is to provide the control method of a programmable controller of having enabled it to employ a flexible password by the user side.
[0020]
[Means for Solving the Problem]A programmable controller which this invention requires for this invention is characterized by that a programmable controller which manages security protection by the input of a password comprises:
A permissive-conditions setting-out means which enables setting out of permissive conditions of an input mistake of the above-mentioned password by a user.
An inhibiting means which forbids registration of the above-mentioned password when an input mistake of the above-mentioned password exceeds permissive conditions set up by the above-mentioned permissive-conditions setting-out means.

[0021]A programmable controller which this invention applies to this invention again is characterized by that a programmable controller which manages security protection by the input of a password comprises:
A restoring condition setting-out means which enables setting out of a restoring condition for receiving a receptionist prohibited state of the above-mentioned password, and returning to a permissive condition by a user.
A release means which cancels a receptionist prohibited state of the above-mentioned password, and is returned to a receptionist permissive condition when a restoring condition set up by the above-mentioned restoring condition setting-out means is fulfilled.

[0022]A control method of a programmable controller concerning this invention, In a control method of a programmable controller of managing security protection by the input of a password, when a user sets up permissive conditions of an input mistake of the above-mentioned password and an input mistake of the above-mentioned password exceeds the above-mentioned permissive conditions, reception of the above-mentioned password is forbidden.
[0023]A control method of a programmable controller concerning this invention, In a control method of a programmable controller of managing security protection by the input of a password, When a restoring condition which a user set up a restoring condition for receiving a receptionist prohibited state of the above-mentioned password, and returning to a permissive condition, and was set up by the above-mentioned restoring condition setting-out means is fulfilled, a receptionist prohibited state of the above-mentioned password is canceled, and it returns to a receptionist permissive condition.
[0024]Here, permissive conditions of the above-mentioned input mistake can be set up by the number of times of an input mistake of the above-mentioned password.
[0025]The above-mentioned restoring condition can be set up in time until it restores in the state of permitting registration of the above-mentioned password, after registration of the above-mentioned password is forbidden.
[0026]
[Embodiment of the Invention]Hereafter, the embodiment of a programmable controller concerning this invention and a method for controlling the same is described in detail with reference to an accompanying drawing.

[0027]Drawing 1 is a block diagram showing the outline composition of the programmable controller concerning this invention.
[0028]In drawing 1, this programmable controller (PLC) 100, MPU (Micro Processing.) Unit101, the internal memory 102, the data memory 103, the system program memory 104, the user program memory 105, bus I/F(bus interface) 106, the display for indication 107, the security protection level setting section 108, and the password input part 109. It connects mutually and comprises the system bath 110.
[0029]Here, MPU101 controls operation by this whole programmable controller 100.
[0030]The internal memory 102 stores the in-house data of the programmable controller 100, and the data memory 103 memorizes various data. The password set as the programmable controller 100 concerning this invention, As a thing peculiar to the programmable controller 100, it may exist in this data memory 103, and may exist in the user program memory 105 as a part of user program.
[0031]The system program of this programmable controller 100 is stored in the system program memory 104, and the user program which the user of this programmable controller 100 uses is stored in the user program memory 105.
[0032]Bus I/F106 interfaces the system bath 110 and an I/O unit, a highly efficient unit, etc. which are not illustrated are connected via this bus I/F106.
[0033]The display for indication 107 comprises LCD (Liquid Crystal Display), and displays the variety of information concerning operation of this programmable controller 100.
[0034]The password input part 109 comprises two or more key switches, and enters a password.
[0035]A permissive-conditions setting-out means by which the security protection level setting section 108 enables setting out of the permissive conditions of the input mistake of a password by a user, And it functions as a restoring condition setting-out means which enables setting out of the restoring condition for receiving the receptionist prohibited state of a password and returning to a permissive condition by a user, and is as [contents / of the setups or restoring condition / concrete] below-mentioned.
[0036]In the programmable controller 100 of this embodiment, Based on the input mistake permissive conditions and the restoring condition of a password which were set up by the user, the security protection of a password is flexibly controlled by the security protection level setting section 108 corresponding to the use of this programmable controller 100.
[0037]The permissive conditions of the input mistake of a password are permissive conditions of the input mistake of the password from the password input part 109, and are set up by the number of times of an input mistake here.
[0038]A restoring condition is set up by time. The time of this restoring condition is that the number of times of an input mistake of the password entered from the password input part 109 exceeds input mistake permissive conditions, It is time until it restores from the time of registration of the password concerned being forbidden in the state, i.e., the state of permitting reinput of a password, of permitting registration of a password again.
[0039]In the programmable controller 100 of this embodiment, the security protection level of this programmable controller 100 is set up in both of the permissive conditions and the restoring condition of the above input mistakes.
[0040]About setting out of the permissive conditions (this embodiment number of times of an input mistake of a password) of an input mistake, setting out which restricts the number of times of an input mistake like unrestricted setting out which does not provide restriction in the number of times of an input mistake or 0 times, 1 time, or 5 times is possible.
[0041]About setting out of a restoring condition (time until it restores in the state of permitting reinput of a password in this embodiment), setting out by non-deer minimum unit time is possible.
[0042]Above setting out of the permissive conditions of an input mistake and setting out of a restoring condition can be arbitrarily performed according to a use by the user side. Therefore, judgment into what thing a security protection level is made is left to the user, and can set up uniquely and freely the arbitrary security protection levels which fitted the use as a user.
[0043]Although a feeling of height of a security protection level is based also on a user's consciousness, the grade and the contents of the level of the security protection level are illustrated below.
[0044]In the programmable controller 100, the permissive conditions of an input mistake are set up indefinitely to set a security protection level as a "low" level. In this case, even if it repeats the input mistake of a password how many times, reinput of a password is possible, and it is suitable when a comparatively low security protection level may be used.
[0045]Setting up the permissive conditions of an input mistake, it sets up a restoring condition in 2 hours 5 times, for example to set a security protection level as an "inside" level. In this case, reinput of a password

becomes impossible when the input mistake of a password is repeated 5 times, In order to make a possible state restore reinput of a password from this state, it must wait for 2 hours, therefore this example is preferred when it needs the security protection level above the above-mentioned example.
[0046]The permissive conditions of an input mistake are set up at once and a restoring condition is set up nothing, for example to set a security protection level as a "quantity" level. In this case, if reinput of a password becomes impossible when the input mistake of a password is performed once, and it will be in this state, even if it waits for how many hours, reinput of a password will not be restored in the possible state. Therefore, this example is preferred when it needs the security protection level above which example of the above.
[0047]Drawing 2 is a flow chart which shows the procedure of the password in the programmable controller 100 shown in drawing 1.
[0048]If a password is entered into this programmable controller 100 in drawing 2 from the password input part 109 shown in drawing 1 (Step 201), This entered password First, the right, i.e., this entered password, The password beforehand set as the data memory 103 or the user program memory 105 of this programmable controller 100 is compared, and it is investigated whether those both are in agreement (Step 202).
[0049]If it is judged here that the password was in agreement (it is YES at Step 202), The lead of the specific user program which the password was received by this programmable controller 100 (Step 207), for example, was stored in the user program memory 105 of this programmable controller 100 is permitted.
[0050]However, if it is judged at Step 202 that a password is not in agreement (it is NO at Step 202) next, it will be investigated whether the number of times of the input mistake whose password does not correspond reached the number of times n of input mistake permission (for example, 5 times) set up by the security protection level setting section 108 (Step 203).
[0051]Here, when it is judged that the input mistake of a password does not amount to n times (it is NO at Step 203), it returns to Step 201 and reinput of a password is permitted.
[0052]However, if the input mistake of a password is judged that it continued repeatedly and the input mistake of the password amounted to n times at Step 203 (it is YES at Step 203), It is investigated whether the release time t which was controlled by the refusal-of-receipt state of the password (Step 204), next was set up by the security protection level setting section 108 passed (Step 205).
[0053]Here, if it is judged that the release time t has not passed (it is NO at Step 205), it will return to Step 205. In the meantime, the refusal-of-receipt state of a password is continued.
[0054]However, at Step 205, when it is judged that the release time t passed (it is YES at Step 205), a password refusal-of-receipt state is canceled (Step 206), it returns to Step 201, and reinput of a password is permitted.
[0055]By the way, the above-mentioned release time t will be reset if the power supply of the programmable controller 100 is turned OFF, and it can also be constituted so that the time check of t hours may be again started after a power turn.
[0056]Drawing 3 is a flow chart which shows the procedure of the password constituted in this way.
[0057]If a password is entered into this programmable controller 100 in drawing 3 from the password input part 109 shown in drawing 1 (Step 301), First, it is investigated whether this entered password of the right, i.e., this entered password, corresponds with the password beforehand set as the data memory 103 of this programmable controller 100 (Step 302).
[0058]If it is judged here that the password was in agreement (it is YES at Step 302), The lead of the specific user program which the password was received by this programmable controller 100 (Step 310), for example, was stored in the user program memory 105 of this programmable controller 100 is permitted.
[0059]However, if it is judged at Step 302 that a password is not in agreement (it is NO at Step 302) next, it will be investigated whether the number of times of the input mistake whose password does not correspond reached the number of times n of permission of the input mistake set up by the security protection level setting section 108 (for example, 5 times) (Step 303).
[0060]Here, when it is judged that the input mistake of a password does not amount to n times (it is NO at Step 303), it returns to Step 301 and reinput of a password is permitted.
[0061]However, if it is judged that the input mistake of the password amounted to n times at Step 303 (it is YES at Step 303), the timer which was controlled by the refusal-of-receipt state of the password (Step 304), next was formed in the programmable controller 100 will be started (Step 305).
[0062]and -- next, the time check of this timer -- it is investigated whether the release time t to which time was set by the security protection level setting section 108 passed (Step 306).
[0063]Here, when it is judged that the release time t passed (it is YES at Step 306), a password refusal-of-receipt state is canceled (Step 309), it returns to Step 301, and reinput of a password is permitted.
[0064]However, a time check will be continued if it is judged that the release time t has not passed at Step 306

(it is NO at Step 306).
[0065]Drawing 4 is a figure which illustrates operation when the power supply of the programmable controller 100 is turned off while performing waiting for progress for t hours at Step 306 of the password procedure shown in above-mentioned drawing 3.
[0066]Although coincidence of a password was not obtained but the timer shown in Step 305 of drawing 3 at the time t1 started in drawing 4, the time check of this timer -- when the power supply of the programmable controller 100 is turned OFF by t2 the time of time not reaching the release time t, it is t3 the time of making a power supply one after that, and the new start of the above-mentioned timer is reset and carried out to an initial value. Therefore, this password is not received even if it enters a password before t4 the time of the release time t passing since t3 the time of making a power supply one.
[0067]And acceptance of a password is attained for the first time after t4 the time of the release time t having passed since t3 the time of making a power supply one..
[0068]Even if according to such composition coincidence of a password is not obtained, but the power supply of this programmable controller 100 is turned OFF for example, for the illegal analysis of a password, it has and it returns, Since the new start of the timer is carried out when a power supply is made one, a password is not received at least between the release time t set up by the security protection level setting section 108.
[0069]
[Effect of the Invention]In the programmable controller which manages security protection by the input of a password according to this invention as explained above, Since it constituted so that a user could set up the security protection level individually according to a user's usage, in the user side, the flexibility of setting out of the level which manages the security protection increases, and the effect that employment of the flexible password set by a user's usage is attained is done so.

[Translation done.]

* NOTICES *

1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DESCRIPTION OF DRAWINGS

[Brief Description of the Drawings]
[Drawing 1]The block diagram showing the outline composition of the programmable controller concerning this invention.
[Drawing 2]The flow chart figure showing the procedure of the password in the programmable controller 100 shown in drawing 1.
[Drawing 3]The flow chart figure showing other procedure of the password in the programmable controller 100 shown in drawing 1.
[Drawing 4]The figure explaining the operation in the case of adopting the procedure of the password shown in drawing 3.
[Drawing 5]The flow chart figure showing the procedure of the password in the conventional programmable controller.
[Description of Notations]
100 Programmable controller (PLC)
101 MPU(Micro Processing Unit)
102 Internal memory
103 Data memory
104 System program memory
105 User program memory
106 bus I/F (bus interface)
107 Display for indication
108 Security protection level setting section
109 Password input part
110 System bath

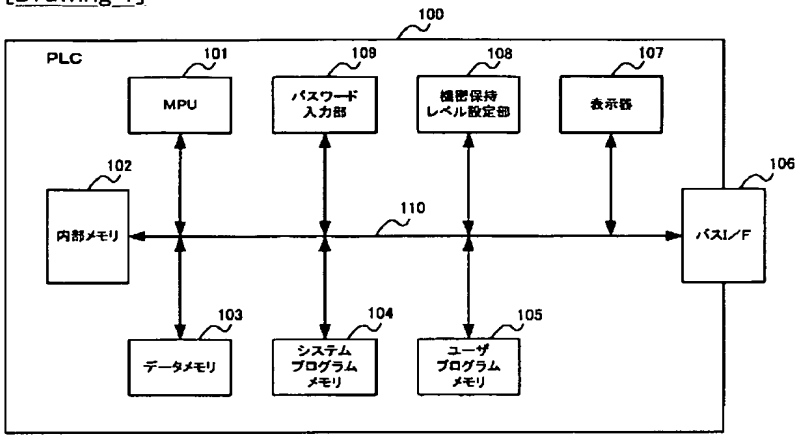
[Translation done.]

* NOTICES *

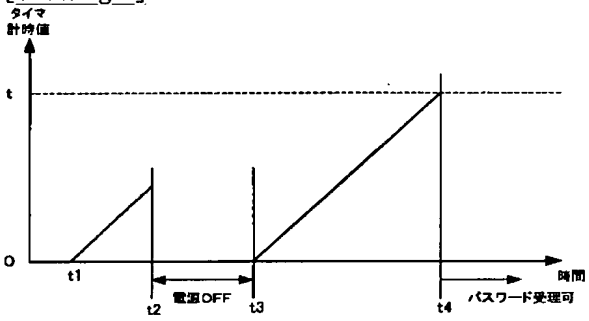
1.This document has been translated by computer. So the translation may not reflect the original precisely.
2.**** shows the word which can not be translated.
3.In the drawings, any words are not translated.

DRAWINGS

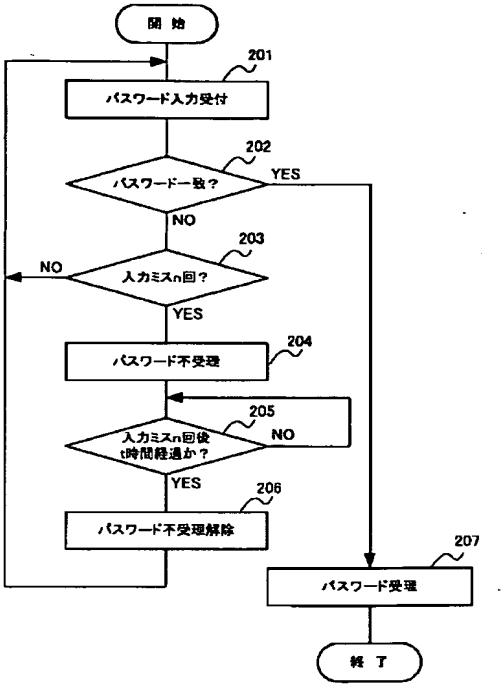
[Drawing 1]



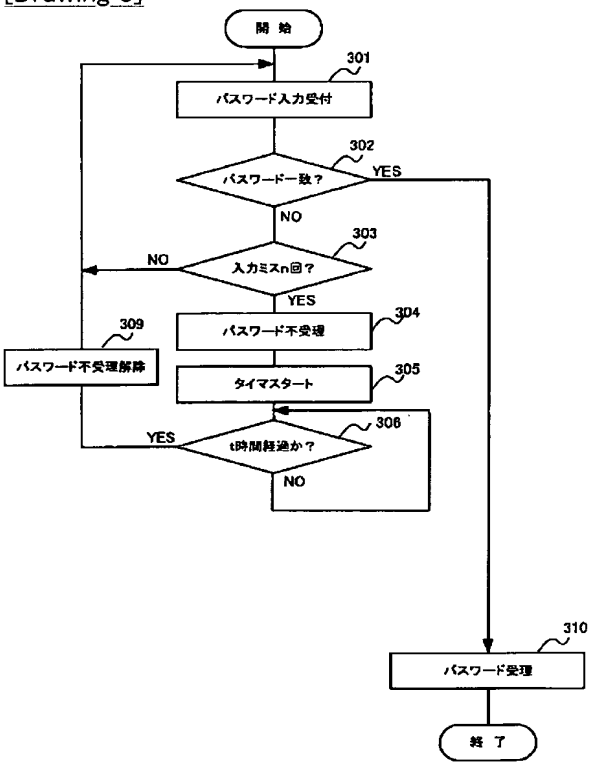
[Drawing 4]



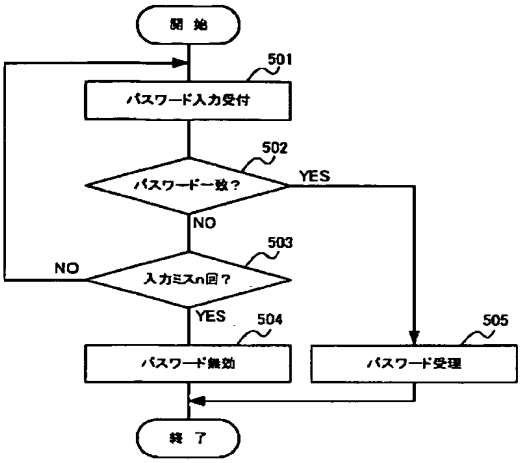
[Drawing 2]



[Drawing 3]



[Drawing 5]



[Translation done.]